BSSi2

Innovations

Review Twice, Implement Once. Doing IT Right the First Time.

3 Ways To Prevent Your Employees From Leaking Confidential Information

A lot of businesses need to come to terms with the fact that their employees are their greatest IT threat. As a business owner, you may be aware of cyberthreats to your business, but your employees might not be. They might not know about the threat of cyber-attacks or malware. They might use unsecured WiFi on company equipment. As a result, your employees may be putting your business at serious risk.

What can you do to change that?

1. It all starts with education. One of the biggest reasons why employees put their employer at risk simply comes down to a lack of education. They don't know about the threats targeting businesses or that small businesses are a major target of hackers and scammers.

You need to do everything you can to train your employees. Give them the education and resources to be a line of defense rather than a risk. Develop a consistent training regimen. If you need to bring in IT professionals to help, do it. Don't make assumptions about critical IT security training if you aren't sure. Professionals can answer your questions and make sure you and your employees have everything you need to know to keep your business secure.

Another important thing is to hold this training regularly. Threats evolve, and you need to stay ahead of the curve. Keep IT security on the minds of your employees. When they forget about it, that's when the risk is highest.

2. Say NO to unsecured, public WiFi. This is a big problem for businesses with remote employees, employees who work from home or employees who use company technology outside of the business walls. According to a Spiceworks study, 61% of employees said they have connected to unsecured WiFi while working remotely.

This is cause for concern. Connecting to public WiFi is like leaving the front door of your home wide-open while posting on social media that you're going to be out of town for a week. You never know who is going to let themselves in and snoop around. Hackers use public hot spots to circulate malware and steal data. Sometimes they even set up fake hot spots with the same name as a legitimate hot spot to trick users into connecting to their WiFi, which makes data theft even easier.

Discouraging your employees from using unsecured, public WiFi is a good step to take, but don't be afraid to take it further. Don't let them connect company equipment to unsecured WiFi at all. And place a bigger focus on endpoint security – make sure your equipment has up-to-date software, malware protection, local firewalls, as well as a VPN (virtual private network). The more layers of security, the better.

3. Protect ALL of your data. Your employees should never save personal or business data on portable/external hard drives, USB drives or even as printed material – and

Continued on the next page...

… Continued from the previous page.

then take that data out of the office. The theft of these types of devices is a real threat. An external hard drive is a tempting target for thieves because they will search the drive for sensitive data, such as financial or customer information that they can use or sell.

If you have remote employees who need to access company data, put a method in place to do just that (it should be discussed as part of your regular company IT security training). They need to know how to properly access the data, save the data or delete it, if necessary. Many businesses go with a secure cloud option, but you need to determine what makes the most sense for your business and its security.

While these three tips are great, nothing beats helping your employees develop a positive IT security mindset. It's all about understanding the threats and taking a proactive approach to security. Proactivity reduces risk. But you don't have to go it alone. Working with experienced IT security professionals is the best way to cover all your bases – and to ensure your employees have everything they need to protect your business.

Facial Recognition Is Going To Get Someone Killed

by Nick Espinosa

It goes without saying that one of the greatest fears most law-abiding people have is being falsely accused of a crime. The imperfect justice system in modern societies, though significantly fairer than previous judicial systems, has resulted in some innocent individuals being falsely imprisoned. The perpetual impetus of any reliable justice system should be to constantly improve on its ability to correctly identify, try and convict only those who are guilty. So, when society starts introducing technology into this evolving system that actually increases the false positive rate of identification, it should terrify us all.

Enter Amazon. This company has been competing in numerous verticals for years now and has entered the facial recognition field with a massive, and aggressive, presence. Dubbed simply "Rekognition," Amazon has been developing this system for years and now, believing it's ready for primetime, has been pushing it to the law enforcement community around the United States with all the vigor of a top salesperson going after the largest bonus in history.

At the moment Rekognition is deployed in an unknown number of police departments around the United States though, according to analysts, that number does nothing but increase. Law enforcement is using this system to help identify suspects in crimes from video they're pulling from various cameras all over their municipalities. Here's the thing though... they've been incorrectly identifying innocent people at an alarming rate.

Facial recognition systems, in their current form, are inherently biased. Studies from MIT have shown that these systems currently favor white males, correctly identifying that demographic with over ninety-nine percent accuracy. When those same systems are applied to women and minorities, those accuracy rates drop up to thirty-five percent. That is around one in three false positive identifications and Amazon's Rekognition is no different in this respect.

In 2018 the ACLU used Rekognition to test the photos of all 535 members of the US Congress against a criminal mugshot database that didn't include their faces. Rekognition identified 28 members of congress as criminals. The ACLU's point was that these systems need serious improvement before they are deployed and used to "identify" suspects. Amazon appears to be working on Rekognition, though it doesn't appear they're working on the actual recognition part since a more recent 2019 test of pictures of California state lawmakers against a criminal mugshot has worse results with 1 in 5 lawmakers being falsely identified as criminals. While the jokes are too easy to make regarding these results, this is no laughing matter to innocent victims of a clearly "not ready for primetime" system being deployed. This hasn't stopped Amazon though and now they're taking these technology multiple

steps further than their competitors can, which is making them all the more attractive to their law enforcement customer base.

For those who didn't know, Amazon recently bought Ring Doorbell. Not without its own alleged cybersecurity and privacy issues, Ring is now being adopted by law enforcement to look for possible crimes in neighborhoods with, or without, the Ring owner's consent. Combine Ring with Rekognition and what Amazon can advertise is the most effective and comprehensive monitoring and identification solution law enforcement has ever seen and it's leveraging the general population to maintain and administer the solution for them. It's a complete win for Amazon, the police and intelligence services that Amazon has close relationships with (Amazon runs a data center for the Central Intelligence Agency and was in the process of winning the contract to host all of the Pentagon's data as well for the next decade).

Not resting on their laurels, Amazon has also been developing a system to identify the intent of the person identified. Currently, Rekognition claims to be able to identify the following emotional states; Happy, Sad, Angry, Surprised, Disgusted, Calm, Confused and Fear. While studies have shown that overwhelmingly people make very similar expressions in emotional states (we all smile when we're overtly happy for example) this too could be a recipe for disaster if there is a gap in its accuracy, not to mention new research that shows our expressions may not be as universal as we think.

Imagine a police officer in a pursuit of a suspect that Rekogintion has "positively" identified and, when cornered, the system identifies the suspect as angry when they're fearful. Does the officer now have a justification for using lethal force on an innocent person? What if the system identified the suspect as sad, or calm, which may lower the officer's guard? There are many questions we cannot take for granted and as we develop wearable technology that will allow law enforcement, and military personnel, to instantly identify others and their emotional states in real time, these are points that must be addressed.

However, the ultimate question for society, regarding this situation, at the moment is simply this: At what point does a facial recognition system become acceptable for public use to ensure safety and what are the privacy implications by allowing it to be pervasively installed or used everywhere? Given the current state of proliferation, answering these questions may be irrelevant at this point. Here's hoping we don't look like anyone else.

This article was written by Nick Espinosa and originally published on smerconish.com, where Nick is a regular columnist. Within hours of publishing this article had tens of thousands of hits and Michael Smerconish himself gave it a shoutout on his morning radio show, so we thought we'd share it with you. https://www.smerconish.com/news/2019/10/1/facial-recognition-is-going-to-get-someone-killed

Michael A. Smerconish is an American radio host and television presenter, newspaper columnist, author, and lawyer. He broadcasts The Michael Smerconish Program weekdays at 9:00 a.m. ET on SiriusXM's POTUS Channel (124), and hosts the CNN and CNN International program Smerconish at 9:00 a.m. ET on Saturdays. He is a Sunday newspaper columnist for The Philadelphia Inquirer. Smerconish has authored seven books: six non-fiction works and one novel. He is also of counsel to the Philadelphia law firm of Kline & Specter.

You can keep up to date with Nick's latest articles by following him online: facebook @NickAEsp | twitter @NickAEsp | Linkedin in/nickespinosa/

On the Lighter Side

October 2019

35 Aztec Court
South Barrington, IL 60010
(312) 752-4679
www.bssi2.com

"We make all of your computer problems go away without the cost of a full-time I.T. staff"

"Like how the people in the story configure their wi-fi?"

Shiny New Gadget of the Month

The Philips Somneo Sleep & Wake-Up Light

Research suggests that when you wake up naturally (that is, you aren't jolted awake by an alarm or radio), you feel more refreshed and energized during the day.

The Philips Somneo Sleep & Wake-Up Light puts this research to the test. It's designed to simulate a natural sunrise right in your bedroom. You can set it to your specific needs, and it will slowly and steadily brighten when you need to wake up. It can also simulate a sunset for the opposite effect when you're going to bed! You can even use the light as a reading lamp — and it has a built-in radio, too!

The Philips Somneo Sleep & Wake-Up Light is a versatile device, perfect for anyone who wants to get a better night's sleep. Find it at Amazon and many other electronic retailers.

Stay up-to-date with the latest Cybersecurity News!

Follow our Chief Security Fanatic and CIO, Nick Espinosa, on social media for cybersecurity videos and articles:

f www.facebook.com/NickAEsp

twitter.com/NickAEsp

in www.linkedin.com/in/nickespinosa/

Follow BSSi2 at:

f www.facebook.com/bssi2

twitter.com/BSSi2llc